ABSTRACT

The present invention proposes an encryption/decryption method able to resist against various attack strategies such as Simple Power Analysis, Timing Analysis or Differential Power Analysis. The method is carried out by a plurality of encryption/decryption modules arranged in series, wherein an encryption/decryption module, different from the first module, starts encryption/decryption operations as soon as said module receives a part of the results of encryption/decryption operations from the immediately preceding encryption/decryption module.